STATEMENT OF
SHARON L PINKERTON
AIRLINES FOR AMERICA®
BEFORE THE
TRANSPORTATION SECURITY SUBCOMMITTEE
OF THE
HOMELAND SECURITY COMMITTEE
OF THE
U.S. HOUSE OF REPRESENTATIVES
FEBRUARY 3, 2015

Airlines for America appreciates the opportunity to express its views about the security measures for employees who are authorized access to secured areas of U.S. airports.

As we discuss more fully below, our members have examined this matter in detail and have identified airport security and employee background check improvements that they believe should be considered. Those include tighter controls over employee access to airport Secured Identification Areas; better communication among law enforcement agencies about investigations of employees who have access to the airport; expansion and harmonization among federal agencies of the crimes that disqualify a person from unescorted access at airports; enhanced risk-based screening of employees; and strengthened employee criminal history record checks.

We believe that the Transportation Security Administration's Aviation Security Advisory Committee is the appropriate venue in which to examine these matters – and any others that may be raised. The ASAC has representatives from a broad spectrum of aviation stakeholders and is the traditional site in which to develop collaboratively proposals to submit for improvements in civil aviation security.

OVERVIEW

The Subcommittee's focus on this issue is both timely and beneficial.

The airline industry regards any breach of civil aviation security as unacceptable. Such breaches need to be carefully examined, root causes identified, and appropriate corrective actions formulated and implemented.

Our members have taken a fresh look at airport security. Below we highlight several possible initiatives concerning employee background checks and airport access practices that we believe should be considered. As noted above, that consideration should be undertaken collaboratively – involving not only the government in its regulatory role but also taking into account the perspectives of airline, airport, vendor and employee representatives.

It is important to provide context to this hearing. The recent security breaches are absolutely unacceptable. That does not change the underlying fact that the aviation security system in our nation is more robust than ever. It is a sophisticated, threat-based system that continues to advance in anticipation of existing and emerging threats. Its success can be attributed in large measure to the methodical application of a risk-based approach to security.

The risk-based security system under which airlines and airports operate has markedly improved security. It is based on the fundamental recognition that sound security policy need not apply the same measures to every individual or item. In other words, one size does not fit all. That recognition is founded on the understanding that not every individual or item poses the same threat to aviation security.

Risk-based security ranks an array of risk factors along a quantitative scale. Once risk levels are determined, security resources are applied in proportion to the assessed risk. In operation, this means that the aviation security system deploys its resources based on individualized assessments of risk of persons (and items) that are subject to the system. Those persons determined to exhibit higher-risk factors receive greater scrutiny. This approach enables us to put resources where they are most needed.

Risk-based security in aviation has been a reality for some time. We thus have considerable, everyday experience with it. For example, the Transportation Security Administration screens about 1.8 million passengers daily using risk-based procedures. We understand risk-based security and we know its effectiveness. We consequently strongly support it. Whatever new measures may emerge concerning airport security, we firmly believe that the commitment of the government and industry to risk-based security must remain undiminished.

Moreover, risk-based security has greatly facilitated TSA's multi-layered security system. As TSA has stated, each layer serves as a protection measure. In combination, these layers create a much stronger, better protected transportation system. That, as experience demonstrates, is the optimum way to confront ever-evolving threats to aviation.

FEDERAL BACKGROUND CHECK REQUIREMENTS FOR AIRLINE EMPLOYEES

Background checks of employees of employees who have unescorted access to secured areas of U.S. airports have been required since 1985. Approval for access to those areas is authorized only if the results of the check indicate that the employee does not have a disqualifying criminal history. There is a basic record-check requirement and separate background check requirements that U.S. Customs and Border Protection and the U.S. Postal Service impose. These distinct requirements are summarized below.

Criminal History Records Check

To ensure that certain designated areas of the airport have controlled access, Secured Identification Areas (SIDA) were established. These are areas on an airport in which only employees who are approved and who have received an airport-issued badge are permitted unescorted access.

A Criminal History Records Check (CHRC) is conducted to determine if an employee should be issued a SIDA badge. The employee seeking such SIDA access must be fingerprinted. Fingerprints are sent to the Federal Bureau of Investigation, which processes them.

The CHRC regulation includes a list of disqualifying crimes that originated in federal legislation. If an employee has a conviction for any of the disqualifying crimes within the last 10 years, he or she will not be approved. If no disqualifying crimes are found in the FBI check, the airport operator notifies the authorizing employer or airline (or other sponsor) that the employee is eligible for a SIDA badge. The employee then goes to a SIDA class to learn the requirements and limitations of access to the SIDA and, upon successfully completing the class, receives an airport-issued ID badge.

U.S. Customs and Border Protection Checks

Employees working at airports where there is international service who need unescorted access to a U.S. Customs and Border Protection-designated security area must receive a CBP-issued seal for her or his identification media.To receive the seal, the employee must meet the qualifications for approval under the CHRC program and not have been convicted of any of 10 additional disqualifying crimes. In addition, CBP may deny an individual a seal if it deems her or him a risk to the public health, interest or safety; national security; or aviation safety. Issuance of a seal also requires a certification by the employer that a “meaningful” background investigation has been conducted and that it has a need for this employee to access the CBP security area.

U.S. Postal Service Checks

Employees who have access to U.S. mail must be approved by a third and separate process. This process is not set forth by law or federal regulation but, rather, through the contractual obligation that the USPS includes in the agreements it has with air carriers to transport mail. The employee must be fingerprinted and the fingerprints are sent to the USPS for review and approval or denial. Virtually any felony conviction within the past 10 years will result in a denial of access to U.S. mail. In addition, the Postal Service’s requirements also include a negative drug test, a separate criminal history check, and legal documentation that the individual has the right to work in the United States.

Airline Vetting

In addition to these criminal history record check programs, TSA regulations require airlines to conduct daily watch list (terrorist database) vetting for all their employees. This is an internal automated process that matches names against the federal watch list that is provided daily.

Additional TSA Actions

Beyond the above-mentioned records checks and vetting, TSA conducts random searches of employees who have access to secured areas of the airport. Moreover, it conducts a Security Threat Assessment of persons who have airport-approved or airport-issued personnel identification media. The assessment includes checks against criminal history records, terrorist watch lists and immigration status.

ADDITIONAL SECURITY MEASURES TO CONSIDER

We believe that the Aviation Security Advisory Committee should evaluate any new airport security measures. ASAC’s mission is to examine areas of civil aviation security with the aim of developing recommendations for the improvement of civil aviation security methods, equipment, and procedures. The consideration of the additional measures that we suggest would fit without difficulty within the ASAC charter. Moreover, the members of are well-equipped to perform this examination and represent a cross section of the airport community. After the ASAC completes its examination, it would forward any recommendations that it developed to the TSA for its action.

These are the areas that we have concluded that the ASAC should examine:

Airports

1. Consider tighter controls over SIDA access control areas based on duty/higher risk times.
2. Consider requiring that local law enforcement agencies notify federal law enforcement agencies, i.e. the FBI and DHS, of any ongoing criminal investigation of an airport employee.

Security Threat Assessments

1. Consider expanding the category of disqualifying crimes and modifying eligibility requirements for employment.
2. Consider expanding current databases that TSA searches.
3. Consider federal standardization of disqualifying crimes.
4. Consider having the federal government specify “permanent disqualifying crimes.” Such crimes, regardless of when they were committed, would prohibit a person from obtaining an airport SIDA badge or aviation employment in a position where he or she would have access to a sensitive security work area.

Employee Screening

1. Consider expanding random screening of employees to include, for example, airport access control entrances and company employee parking lots.
2. Consider developing a program to identify high- and low-risk airport community employees.
    a. Those employees identified as low-risk would be subjected to a risk-based screening approach.
    b. Higher-risk employees would undergo random screening more frequently, based on risk and location.

Criminal History Records Checks

The FBI’s initial criminal history records check /fingerprint check is only conducted at the time of employment. It has a 10 year “look back”. There is no ongoing vetting after the initial review. The industry is unable under the existing system to perform updated or random checks without again collecting fingerprints from the employee and preforming a new CHRC. In view of this situation, we suggest that:

1. Consideration be given to enabling airports and airlines to perform random/specific CHRC without recollecting fingerprints in the event that suspicious activities are observed.
2. Consideration be given to lengthening the “look back” period for criminal history checks-- e.g., 18-20 years.

Furthermore, there is no current system to inform employers should an employee be charged with a crime after the criminal history records check.

1. For example, if an employee hired in Virginia is arrested in Nevada, the employer would only know of the arrest if the employee self-disclosed the arrest.
2. Consideration should be given to having the FBI conduct recurrent criminal history record checks and notification be provided to the airport/airline and/or other law-enforcement agency for follow up.

Airlines

As mentioned above, TSA requires airlines to conduct daily watch list (terrorist database) vetting of all employees. That process can be made more efficient.

1. Consideration should be given to the TSA creating a web portal whereby employers can examine new-hire employees.
   a. Employers could populate the web site with complete employee lists for perpetual vetting against the watch list.
   b. Watch list vetting of employees would then shifted from the industry to TSA responsibility, which would be a more sensible allocation of this responsibility.

This is not an exhaustive list. Other possible initiatives can be added to it.

****

We believe that the foregoing response would be the most advantageous way to examine potential changes to criminal history record check, vetting and airport access measures. It would assure broad-based stakeholder input by using the longstanding ASAC. Any recommendations that were forthcoming should be mindful of the risk-based framework of current aviation security. TSA, of course, would have the ultimate authority to dispose of the recommendations.